



UNITED STATES ATTORNEY'S OFFICE
Southern District of New York

U.S. ATTORNEY PREET BHARARA

FOR IMMEDIATE RELEASE
Tuesday, May 28, 2013
<http://www.justice.gov/usao/nys>

CONTACT: U.S. ATTORNEY'S OFFICE
Press Office
(212) 637-2600

DOJ
Press Office
(202) 514-2007

SECRET SERVICE
Press Office
(718) 840-1132

IRS-CI
Press Office
(202) 515-4013

ICE HSI
Press Office
(646) 230-3289

**MANHATTAN U.S. ATTORNEY ANNOUNCES CHARGES AGAINST
LIBERTY RESERVE, ONE OF WORLD'S LARGEST DIGITAL
CURRENCY COMPANIES, AND SEVEN OF ITS PRINCIPALS AND
EMPLOYEES FOR ALLEGEDLY RUNNING A \$6 BILLION MONEY
LAUNDERING SCHEME**

*Liberty Reserve Allegedly Processed at Least 55 Million Illegal Transactions for at Least One
Million Users Worldwide Facilitating Global Criminal Conduct*

*Investigation and Takedown Believed to Be the Largest International Money Laundering
Prosecution in History, Involving Law Enforcement Actions in 17 Countries*

Preet Bharara, the United States Attorney for the Southern District of New York, Mythili Raman, the Acting Assistant Attorney General for the Criminal Division of the U.S. Department of Justice ("DOJ"), Steven G. Hughes, the Special Agent-in-Charge of the New York Office of the U.S. Secret Service, Richard Weber, the Chief of the Internal Revenue Service, Criminal Investigation ("IRS-CI"), and James T. Hayes, Jr., the Special Agent-in-Charge of the New York Field Office of the U.S. Immigration and Customs Enforcement's ("ICE") Homeland Security Investigations ("HSI"), announced today the unsealing of an indictment charging LIBERTY RESERVE, a company that operated one of the world's most widely used digital currency services, and seven of its principals and employees with money laundering and operating an unlicensed money transmitting business. LIBERTY RESERVE is alleged to have had more than one million users worldwide, including more than 200,000 users in the U.S, who conducted approximately 55 million transactions – virtually all of which were illegal – and laundered more than \$6 billion in suspected proceeds of crimes including credit card fraud, identity theft, investment fraud, computer hacking, child pornography, and narcotics trafficking.

Five defendants were arrested on May 24, 2013, including ARTHUR BUDOVSKY, the principal founder of LIBERTY RESERVE, who was arrested in Spain; VLADIMIR KATS, the co-founder of LIBERTY RESERVE, who was arrested in Brooklyn, New York; AZZEDDINE EL AMINE, a manager of LIBERTY RESERVE's financial accounts, who was arrested in Spain; and MARK MARMILEV and MAXIM CHUKHAREV, who helped design and maintain LIBERTY RESERVE's technological infrastructure, who were arrested in Brooklyn, New York, and Costa Rica, respectively. Two other defendants, AHMED YASSINE ABDELGHANI ("YASSINE") and ALLAN ESTEBAN HIDALGO JIMENEZ ("HIDALGO"), are at large in Costa Rica.

In addition to the criminal charges brought in the Indictment, five domain names were seized, namely, the domain name of LIBERTY RESERVE and the domain names of four exchanger websites that were controlled by one or more of the defendants; 45 bank accounts were restrained or seized; and a civil action was filed against 35 exchanger websites (see attached list) seeking the forfeiture of the exchangers' domain names because the websites were used to facilitate the LIBERTY RESERVE money laundering conspiracy and constitute property involved in money laundering. The four exchangers whose domain names were seized, as well as the 35 exchangers whose domain names are the subjects of the civil forfeiture action, were all exchangers that transacted business with LIBERTY RESERVE and were listed on LIBERTY RESERVE's website as "pre-approved exchangers." The investigation and takedown involved law enforcement action in 17 countries, including Costa Rica, the Netherlands, Spain, Morocco, Sweden, Switzerland, Cyprus, Australia, China, Norway, Latvia, Luxembourg, the United Kingdom, Russia, Canada, and the U.S.

In a coordinated action, the U.S. Department of the Treasury and its Financial Crimes Enforcement Network today announced that LIBERTY RESERVE has been named as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act. This action includes a notice to the Federal Register proposing to prohibit covered U.S. financial institutions from opening or maintaining correspondent or payable-through accounts for foreign banks that are being used to process transactions involving LIBERTY RESERVE.

Manhattan U.S. Attorney Preet Bharara said: "As alleged, the only liberty that Liberty Reserve gave many of its users was the freedom to commit crimes – the coin of its realm was anonymity, and it became a popular hub for fraudsters, hackers, and traffickers. The global enforcement action we announce today is an important step towards reining in the 'Wild West' of illicit Internet banking. As crime goes increasingly global, the long arm of the law has to get even longer, and in this case, it encircled the earth."

Acting Assistant Attorney General Mythili Raman said: "As charged, Liberty Reserve operated, on an enormous scale, a digital currency system designed to provide cyber and other criminals with a way to launder their profits without leaving a trace. The company's very purpose was to launder its users' criminal proceeds through the U.S. and global financial system. By indicting Liberty Reserve and its principals, restraining over \$25 million in criminal proceeds, forfeiting domain names, and seizing servers in countries around the globe, our message is clear: money launderers can run, but they can't hide from the U.S. justice system. Combating the threat of global illicit finance requires using every tool we have at our

disposal, and today we demonstrate our resolve to ensure that criminals who exploit the U.S. and global financial system will be held to account.”

Secret Service Special Agent-in-Charge Steven G. Hughes said: “These arrests are an example of the Secret Service’s commitment to investigate and apprehend criminals engaged in the misuse of virtual currencies to conduct global monetary fraud. Cyber criminals should be reminded today that they are unable to hide behind the anonymity of the Internet to avoid regulated financial systems. We are grateful to our many law enforcement partners throughout the world for assistance in this investigation, especially in Costa Rica, Spain and the Netherlands.”

IRS-CI Chief Richard Weber said: “We are now entering the cyber age of money laundering. Technology advancements over the past several years have dramatically increased opportunities for criminals to move, conceal and enjoy their ill-gotten gains. Liberty Reserve and its principals have been charged with operating a sophisticated and complex system for structuring financial transactions which catered to those engaged in such criminal activity. What they did not anticipate was our robust partnerships with domestic and foreign law enforcement that allowed us collectively to follow the cyber money trail in the United States and around the world.”

ICE HSI Special Agent-in-Charge James T. Hayes, Jr. said: “The actions of the U.S. Secret Service, IRS, and HSI in dismantling the Liberty Reserve operation are critical because transnational criminal organizations can succeed only so long as they can funnel their illicit proceeds freely and without detection. HSI is proud of its partnership through the Global Illicit Financial Team and will continue to aggressively target financial institutions that deliberately enable businesses and individuals to evade global financial systems in furtherance of criminal schemes.”

According to the allegations in the Indictment, the Civil Forfeiture Complaint, and other documents filed in Manhattan federal court:

Background

LIBERTY RESERVE was incorporated in Costa Rica in 2006 and operated the digital currency commonly referred to as “LR.” While the company billed itself as the Internet’s “largest payment processor and money transfer system,” serving “millions” of people around the world, including the U.S., at no time did the company register with the U.S. Department of the Treasury as a money transmitting business, as required by law.

BUDOVSKY, the principal founder of LIBERTY RESERVE, directed and supervised its operations, finances, and corporate strategy. KATS, a co-founder, helped operate the company until 2009. The day-to-day operations of LIBERTY RESERVE were managed, at different times, by HIDALGO and YASSINE. EL AMINE managed various financial accounts controlled by LIBERTY RESERVE, while MARMILEV and CHUKHAREV were primarily responsible for designing and maintaining the company’s technological infrastructure.

Overview of Liberty Reserve's Money Laundering Operation

The defendants created, structured, and operated LIBERTY RESERVE as a criminal bank-payment processor designed to help users conduct illegal transactions anonymously and launder the proceeds of their crimes. It emerged as one of the principal money transfer agents used by cyber criminals around the world to distribute, store, and launder the proceeds of their illegal activity. The company grew into a financial hub of the cybercrime world, facilitating a broad range of online criminal activity, including credit card fraud, identity theft, investment fraud, computer hacking, child pornography, and narcotics trafficking. LIBERTY RESERVE was used extensively for illegal purposes, functioning as the bank of choice for the criminal underworld because it provided an infrastructure that enabled cyber criminals around the world to conduct anonymous and untraceable financial transactions.

The defendants also protected the criminal infrastructure of LIBERTY RESERVE by, among other things, lying to anti-money laundering authorities in Costa Rica and pretending to shut down LIBERTY RESERVE after learning the company was being investigated by U.S. law enforcement. They then continued operating the business through a set of shell companies, and moved tens of millions of dollars through shell company accounts maintained in Cyprus, Russia, China, Hong Kong, Morocco, Spain, Australia, and elsewhere.

The Criminal Design of Liberty Reserve

In order to use LR currency, a user first had to open an account through the LIBERTY RESERVE website and provide basic identifying information. Unlike traditional banks or legitimate online processors, LIBERTY RESERVE did not require users to validate their identities. Users routinely established accounts under false names, including such blatantly criminal names as "Russia Hackers" and "Hacker Account." As part of the investigation, a law enforcement agent opened and executed transactions through an undercover account at LIBERTY RESERVE in the name of "Joe Bogus" and the address "123 Fake Main Street" in "Completely Made Up City, New York."

Once an account was established, the user could conduct transactions with other LIBERTY RESERVE users. In these transactions, the user could receive transfers of LR from other users' accounts, and transfer LR from his or her own account to other users, including any "merchants" that accepted LR as payment. LIBERTY RESERVE charged a one-percent fee up to a maximum of \$2.99, every time a user transferred LR to another user through the LIBERTY RESERVE system. For an additional "privacy fee" of 75 cents per transaction, a user could hide his or her own LIBERTY RESERVE account number when transferring funds, effectively making the transfer completely untraceable, even within LIBERTY RESERVE's already opaque system.

To add an additional layer of anonymity, LIBERTY RESERVE did not permit users to fund their accounts by transferring money to the company directly through a credit card transfer or other means. Users also could not withdraw funds from their accounts directly. Instead, LIBERTY RESERVE users were required to make any deposits or withdrawals through the use of third-party "exchangers," which enabled the company to avoid collecting any information about its users through banking transactions or other activity that would leave a centralized

financial paper trail. BUDOVSKY, KATS, and EL AMINE owned and operated certain LIBERTY RESERVE exchanger services.

The LIBERTY RESERVE website recommended a number of “pre-approved” exchangers, which tended to be unlicensed money transmitting businesses operating in countries without significant governmental money laundering oversight or regulation, such as in Malaysia, Russia, Nigeria, and Vietnam. The exchangers charged transaction fees for their services that were much higher than the fees charged by mainstream banks or payment processors for comparable money transfers.

The Criminal Use of Liberty Reserve

To further enable the use of LIBERTY RESERVE for criminal activity, its website offered a “shopping cart interface” that “merchant” websites could use to accept LR currency as a form of payment. The “merchants” who accepted LR currency were overwhelmingly criminal in nature. They included traffickers of stolen credit card data and personal identity information, peddlers of various types of online Ponzi and get-rich-quick schemes, computer hackers for hire, unregulated gambling enterprises, and underground drug-dealing websites.

In addition to being used to process payments for illegal goods and services online, LIBERTY RESERVE was also used by cyber criminals to launder criminal proceeds and transfer funds among criminal associates. For example, LIBERTY RESERVE was used by credit-card theft and computer-hacking rings operating in countries around the world, including Vietnam, Nigeria, Hong Kong, China, and the U.S., to distribute proceeds of these conspiracies among the members involved.

The defendants were well aware that LIBERTY RESERVE functioned as an unlawful money-laundering enterprise. In an online chat between KATS and YASSINE that was captured by law enforcement, KATS explicitly described LIBERTY RESERVE’s activities as “illegal” and noted that “everyone in USA” such as “DOJ” knows “LR is [a] money laundering operation that hackers use.”

* * *

LIBERTY RESERVE, BUDOVSKY, 39, a citizen of Costa Rica who resides in the Netherlands, KATS, 41, of Brooklyn, New York, YASSINE, 42, of Costa Rica, HIDALGO, 28, of Costa Rica, EL AMINE, 46, of Costa Rica, MARMILEV, 33, of Brooklyn, New York, and CHUKHAREV, 27, of Costa Rica, are each charged with one count of conspiracy to commit money laundering, which carries a maximum term of 20 years in prison, one count of conspiracy to operate an unlicensed money transmitting business, which carries a maximum term of five years in prison, and operation of an unlicensed money transmitting business, which carries a maximum term of five years in prison. The terms of incarceration apply to the individual defendants.

Mr. Bharara praised the outstanding investigative work of the Secret Service, the IRS-CI, and ICE HSI, which worked together in this case as part of the Global Illicit Financial Team. He also thanked the Secret Service’s New York Electronic Crimes Task Force for their

extraordinary assistance with the investigation. Additionally, Mr. Bharara specially thanked all the international law enforcement agencies that assisted this investigation, in particular, the Judicial Investigation Organization in Costa Rica, the National High Tech Crime Unit in the Netherlands, the Spanish National Police, Financial and Economic Crime Unit, the Cyber Crime Unit at the Swedish National Bureau of Investigation, and the Swiss Federal Prosecutor’s Office. Mr. Bharara also thanked the Shadowserver Foundation for acting as the hosting provider for the domain names that were seized pursuant to the Court-authorized seizure warrants.

This case is being prosecuted jointly with the Department of Justice’s Asset Forfeiture and Money Laundering Section (“AFMLS”), which is overseen by Acting Assistant Attorney General Mythili Raman. Mr. Bharara thanked AFMLS for its partnership and also thanked the Department of Justice’s Office of International Affairs and Computer Crime and Intellectual Property Section for their support.

If you believe you were a victim of a crime and were defrauded of funds through the use of Liberty Reserve, and you wish to provide information to law enforcement and/or receive notice of future developments in the case or additional information, please contact (888) 238-0696 or (212) 637-1583.

The prosecution of this case is being handled by the Office’s Complex Frauds Unit and Asset Forfeiture Unit.

The charges contained in the Indictment are merely accusations and the defendants are presumed innocent unless and until proven guilty.

13-192

###

Exchanger Domain Names Subject to Civil Forfeiture Complaint

WM-CENTER.COM	MEWAHGOLD.COM
E-NAIRA.COM	CENTREGOLD.CA
ECARDONE.COM	ELECTRUMX.COM
EBUYGOLD.COM	TUKARUID.COM
GETEMONEY.COM	ENTELNOVA.COM
EPAYMONSTER.COM	TACOAUTHORIZED.COM
INSTANTGOLDNG.COM	INTEXCHANGE.COM
JTGOLD.COM	UKRNETMONEY.COM
GOLDNAIRAEXCHANGE.COM	WMIRK.COM
SUPERCHANGE.RU	NIGERIAGOLDEXCHANGER.COM
WEBMONEY.CO.NZ	EDEALSPOT.COM
M-GOLD.COM	DUYDUYCHANGER.COM
GOLDMEDIATOR.COM	MAGNETIC-EXCHANGE.COM
ABSOLUTEXCHANGE.EU	MONEYEXCHANGE.VN
ABC-EX.NET	MI-BILLETERA.COM
NICCIEXCHANGE.COM	EXHERE.COM
ALERTEXCHANGER.COM	VELAEXCHANGE.COM
GOLDEXPAY.COM	